1   Claim 1 (currently amended): A computer-implemented method of provisioning an aggregated

2   service in a computing network, comprising steps of:

3   obtaining credentials of a user who requests to access an aggregated service;

4   locating, in a network-accessible registry, a service description document specifying a

5   provisioning interface for the aggregated service, the aggregated service comprising an

6   aggregation of a plurality of sub-services and the provisioning interface specifying how to invoke

7   identity functions of the aggregated service;

8   analyzing the obtained credentials by invoking one or more of the identity functions,

9   according to the specification thereof in the provisioning interface, to determine whether the user

10   is authenticated for, and/or is authorized for, accessing the aggregated service; [[and]]

11   allowing the user to access the aggregated service only if the analyzing step has a

12   successful result<u>; and</u>

13   <u>programmatically relaying identity information obtained by invoking one or more of the</u>

14   <u>identity functions among at least two of the sub-services of the aggregated service</u>.

1   Claim 2 (currently amended): The computer-implemented method according to Claim 1, wherein

2   an implementation of each of the ~~identify~~ <u>identity</u> functions of the aggregated service is provided

3   by at least one of the sub-services.

1   Claim 3 (previously presented): The computer-implemented method according to Claim 1,

2   wherein:

3   at least one of the sub-services has a local provisioning interface, the local provisioning

4   interface specified in a corresponding service description document and comprising a specification

5   of how to invoke one or more identity functions of the sub-service; and

6   the identity functions in the provisioning interface of the aggregated service are selected

7   from the local provisioning interfaces; and further comprising the step of:

8   controlling access to each of the sub-services having the local provisioning interface,

9   further comprising the steps of:

10   determining whether the user is authenticated for, and/or authorized for, accessing

11   the sub-service by invoking at least one of the one or more identity functions of the sub-service,

12   according to the specification thereof in the local provisioning interface; and

13   allowing the user to access the sub-service only if the determining step has a

14   successful result.

1   Claim 4 (previously presented): The computer-implemented method according to Claim 3,

2   wherein:

3   the step of obtaining credentials of the user also obtains sub-service credentials for at least

4   one of the sub-services having the local provisioning interface; and

5   the determining step uses the obtained sub-service credentials.

1   Claim 5 (currently amended): <u>A computer-implemented method of provisioning an aggregated</u>

2   <u>service in a computing network, comprising steps of:</u> ~~The computer-implemented method~~

3   ~~according to Claim 1,~~

4   locating, in a network-accessible registry, a service description document specifying a

5   provisioning interface for an aggregated service, the aggregated service comprising an

6   aggregation of a plurality of sub-services and the provisioning interface specifying how to invoke

7   identity functions of the aggregated service, wherein[[:]] one or more operations of at least one of

8   the sub-services is access-protected;

9   ~~the obtaining step further comprises~~ obtaining, for at least one of the access-protected

10   operations, operation-specific credentials of [[the]] a user who requests to access the aggregated

11   service; and ~~further comprising the step of:~~

12   controlling access to each of at least one of the access-protected operations, further

13   comprising the steps of:

14   analyzing the obtained operation-specific credentials by invoking one of more of

15   the identity functions, according to the specification thereof in the provisioning interface, to

16   determine whether the user can access the access-protected operation; and

17   allowing the user to access the access-protected operation only if the step of

18   analyzing the obtained operation-specific credentials ~~has a successful result~~ determines that the

19   user can access the access-protected operation.

Claims 6 - 7 (canceled)

1   Claim 8 (currently amended): The computer-implemented method according to Claim [[7]] 1,

2   wherein the programmatic relaying comprises sending a message which specifies the identity

3   information in a header of the message and which specifies a service request in a body of the

4   message.

1   Claim 9 (previously presented): The computer-implemented method according to Claim 8,

2   wherein the message is a SOAP ("Simple Object Access Protocol") message.

1   Claims 10 - 11 (canceled)

1   Claim 12 (currently amended): The computer-implemented method according to Claim [[2]] <u>5</u>,

2   wherein the <u>service description document in the</u> network-accessible registry is <u>located</u> ~~accessed~~

3   using standardized messages.

1   Claim 13 (currently amended): A system for provisioning an aggregated service in a computing

2   network, comprising:

3   ~~means for defining a provisioning interface of the aggregated service;~~

4   ~~means for specifying the provisioning interface in a service description document;~~

5   means for obtaining credentials of a user who requests to access an aggregated service;

6   means for locating, in a network-accessible registry, a service description document

7   specifying a provisioning interface for the aggregated service, the aggregated service comprising

8   an aggregation of a plurality of sub-services and the provisioning interface specifying how to

9   invoke identity functions of the aggregated service<u>, wherein the service description document is</u>

10   <u>specified in a Web Services Description Language ("WSDL") markup language</u>;

11   means for analyzing the obtained credentials by invoking one or more of the identity

12   functions, according to the specification thereof in the provisioning interface, to determine

13   whether the user is authenticated for, and/or is authorized for, accessing the aggregated service;

14   and

15   means for allowing the user to access the aggregated service only if the means for

16   analyzing has a successful result.

1   Claim 14 (currently amended): A computer program product for provisioning an aggregated

2   service in a computing network, the computer program product embodied on one or more

3   computer-readable media and comprising:

4   computer-readable program code [[means]] for obtaining credentials of a user who

5   requests to access an aggregated service;

6   computer-readable program code [[means]] for locating, in a network-accessible registry,

7   a service description document specifying a provisioning interface for the aggregated service, the

8   aggregated service comprising an aggregation of a plurality of sub-services and the provisioning

9   interface specifying how to invoke identity functions of the aggregated service;

10   computer-readable program code [[means]] for analyzing the obtained credentials by

11   invoking one or more of the identity functions, according to the specification thereof in the

12   provisioning interface, to determine whether the user is authenticated for, and/or is authorized for,

13   accessing the aggregated service, wherein an implementation of at least one of the sub-services is

14   located dynamically, at run-time; and

15   computer-readable program code [[means]] for allowing the user to access the aggregated

16   service only if the computer-readable program code [[means]] for analyzing has a successful

17   result.

Claim 15 (canceled)

1   Claim 16 (currently amended): The method according to Claim [[7]] 1, wherein the identity

2   information is initially obtained as a result of the analyzing step.

1   Claim 17 (currently amended): The method according to Claim [[7]] 1, wherein the identity

2   information comprises an authentication token generated by one of the invoked identity functions.

1   Claim 18 (currently amended): A [[The]] computer-implemented method according to Claim 1

2   for provisioning an aggregated service in a computing network, comprising steps of:

3   obtaining credentials of a user who requests to access an aggregated service;

4   locating, in a network-accessible registry, a service description document specifying a

5   provisioning interface for the aggregated service, the aggregated service comprising an

6   aggregation of a plurality of sub-services and the provisioning interface specifying how to invoke

7   identity functions of the aggregated service, wherein:

8   at least two of the sub-services each have associated therewith an identity system

9   for access control thereto;

10   at least two of the associated identity systems are heterogeneous; and

11   at least one selected one of the identity functions of the aggregated service enables

12   dynamically joining at least two of the heterogeneous identity systems;

13   analyzing the obtained credentials by invoking one or more of the identity functions,

14   according to the specification thereof in the provisioning interface, to determine whether the user

15   is authenticated for, and/or is authorized for, accessing the aggregated service; and

16   allowing the user to access the aggregated service only if the analyzing step determines

17   that the user is authenticated for, and/or is authorized for, accessing the aggregated service.

1   Claim 19 (previously presented): The method according to Claim 18, wherein the at least one

2   selected identity function, upon invocation, identifies the identity system that stores information

3   pertaining to users of the sub-service with which that identity system is associated.

1   Claim 20 (previously presented): The method according to Claim 19, wherein the dynamic

2   joining is enabled by relaying the identification of the identity system among the dynamically-

3   joined identity systems.